

1/22

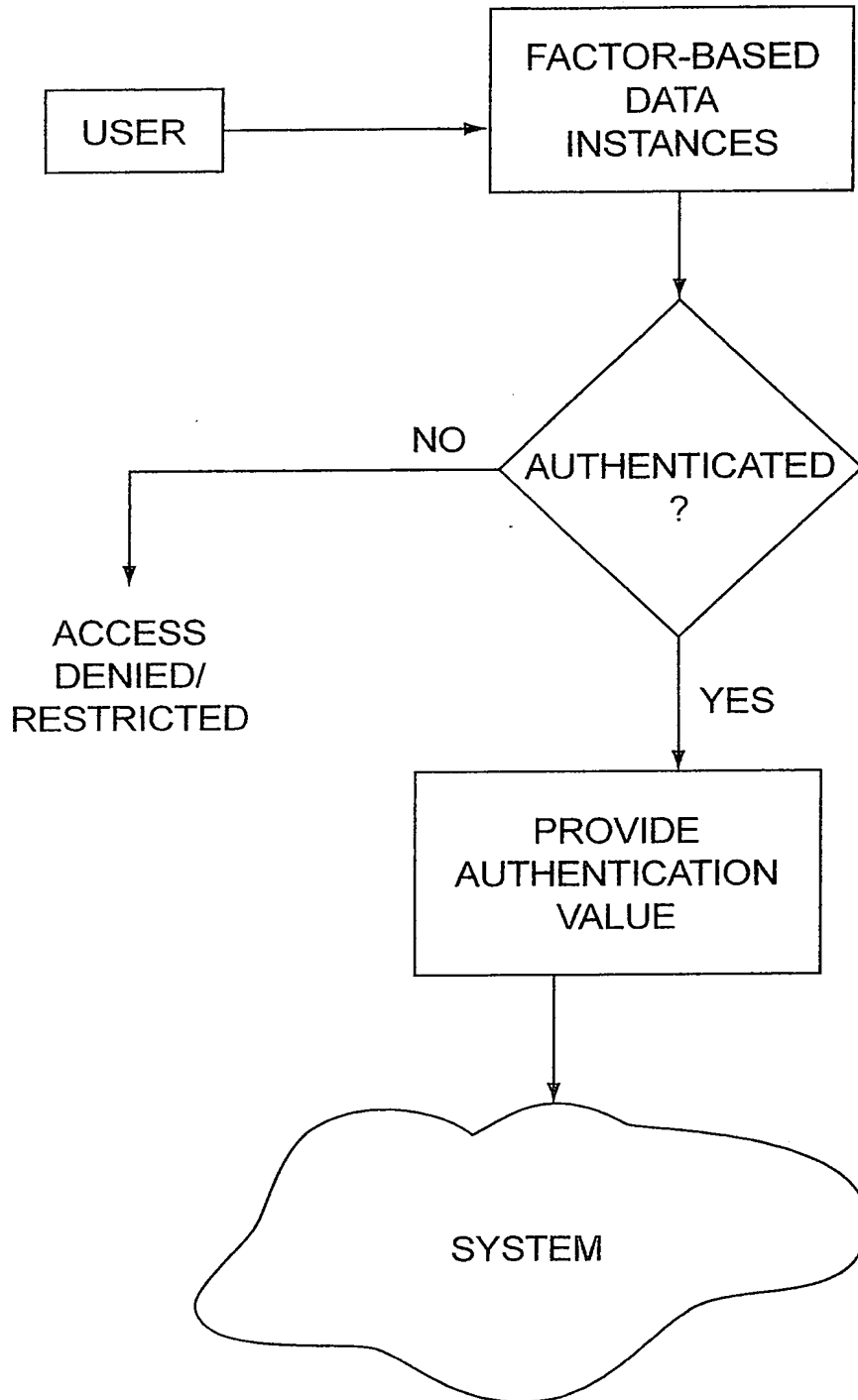


FIG. 1

2/22

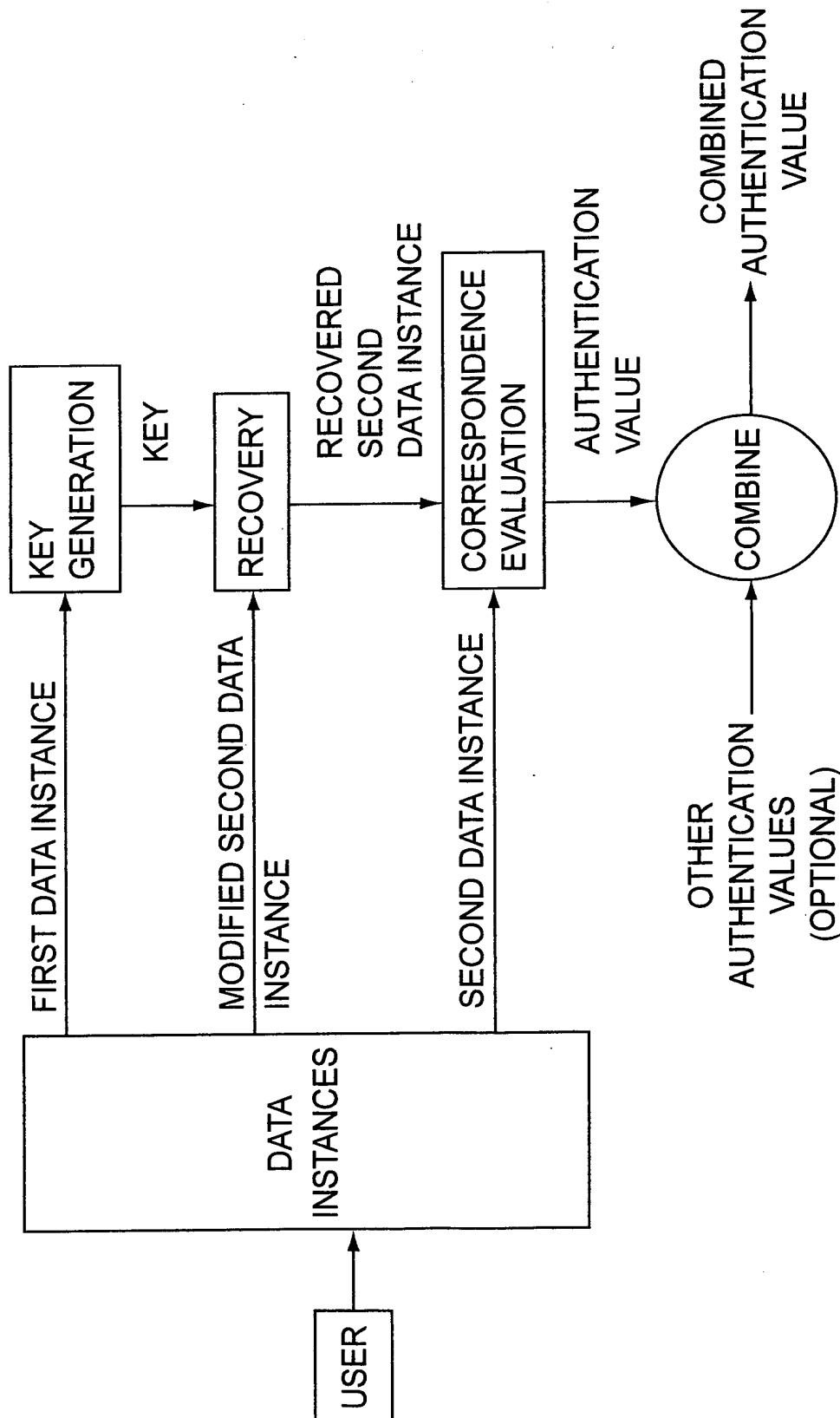


FIG. 2

3/22

MULTI-FACTOR MEMBER IDENTIFICATION (ENCRYPTED SN + FINGERPRINT)

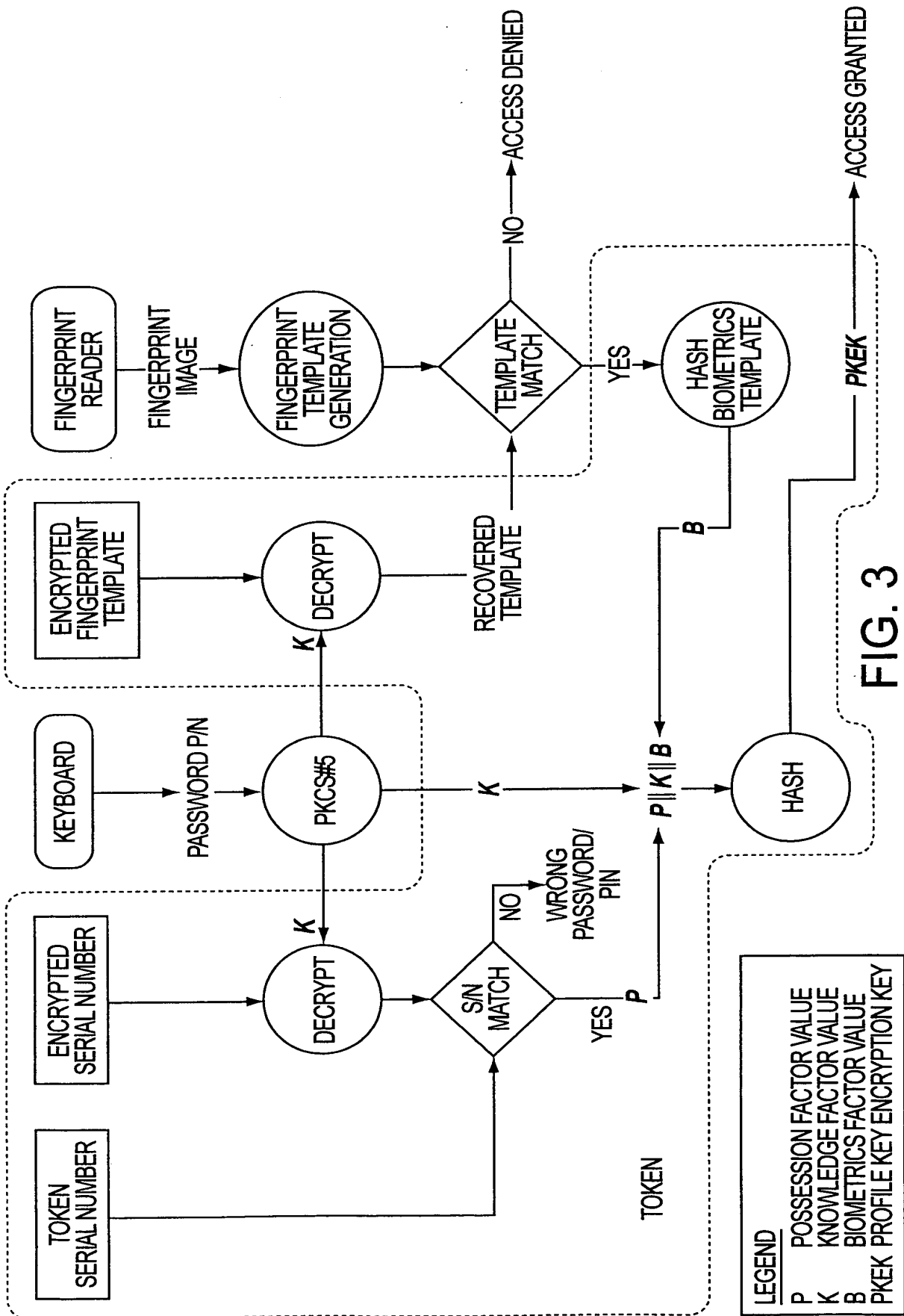
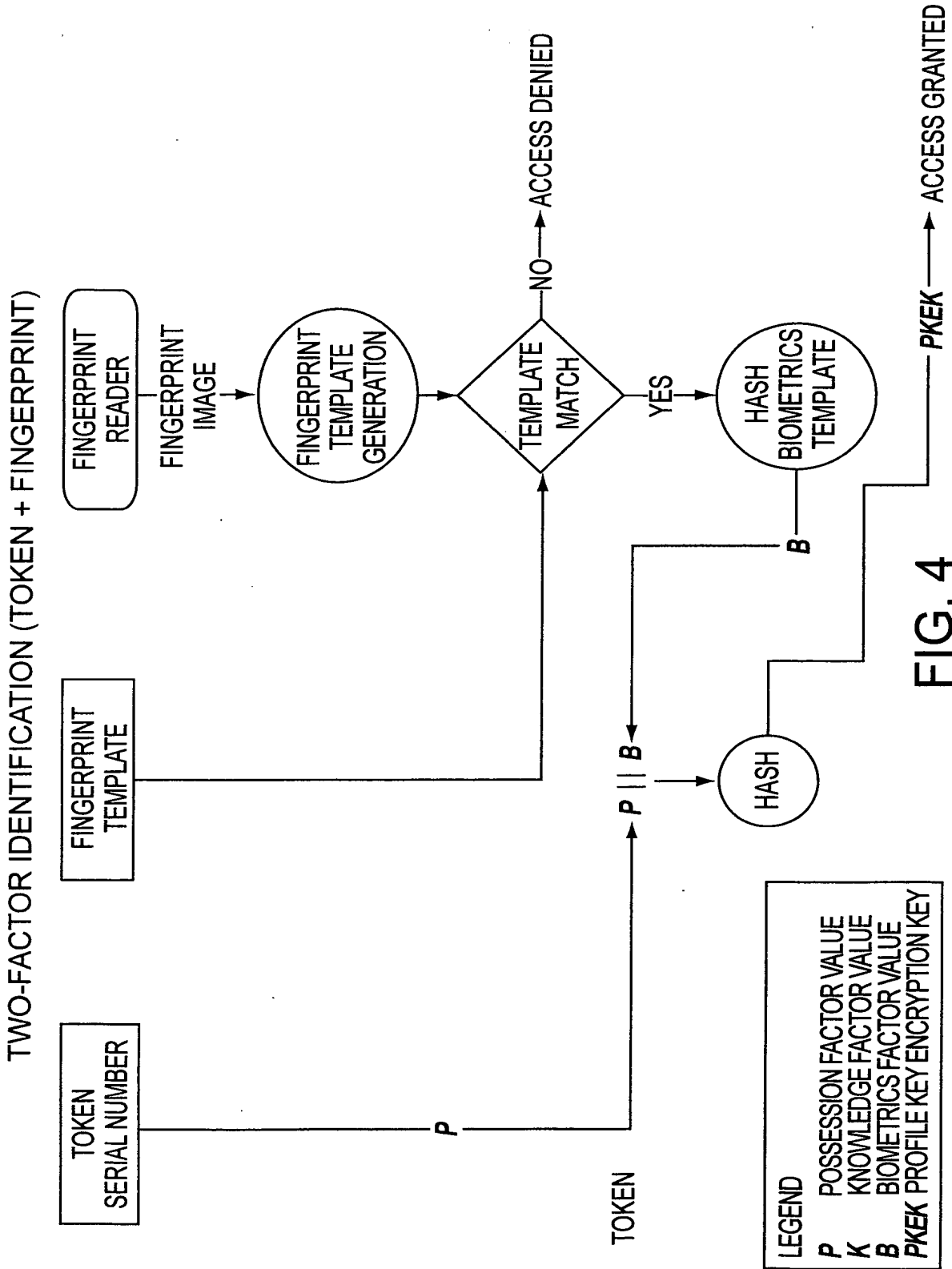
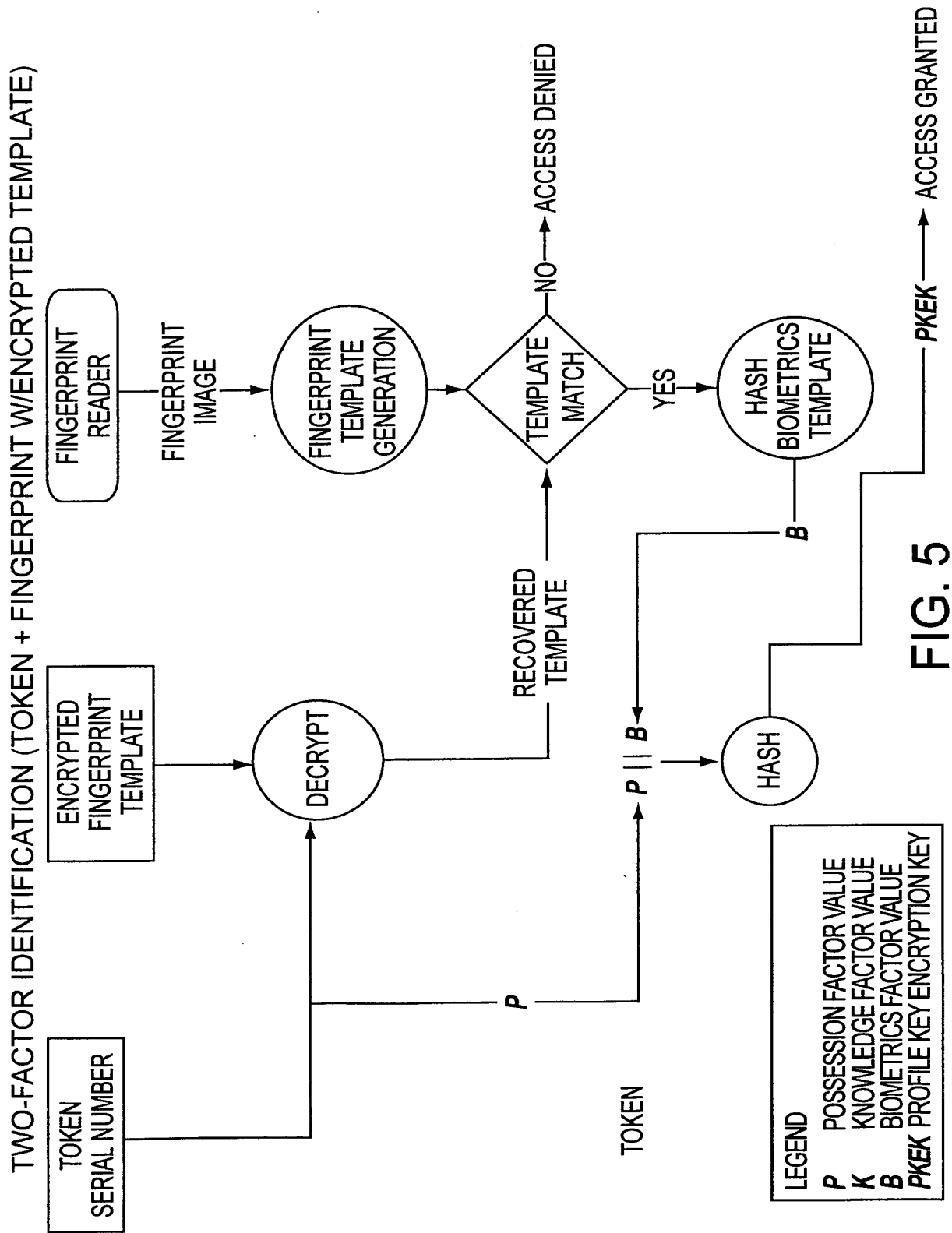


FIG. 3

4/22



5/22



6/22

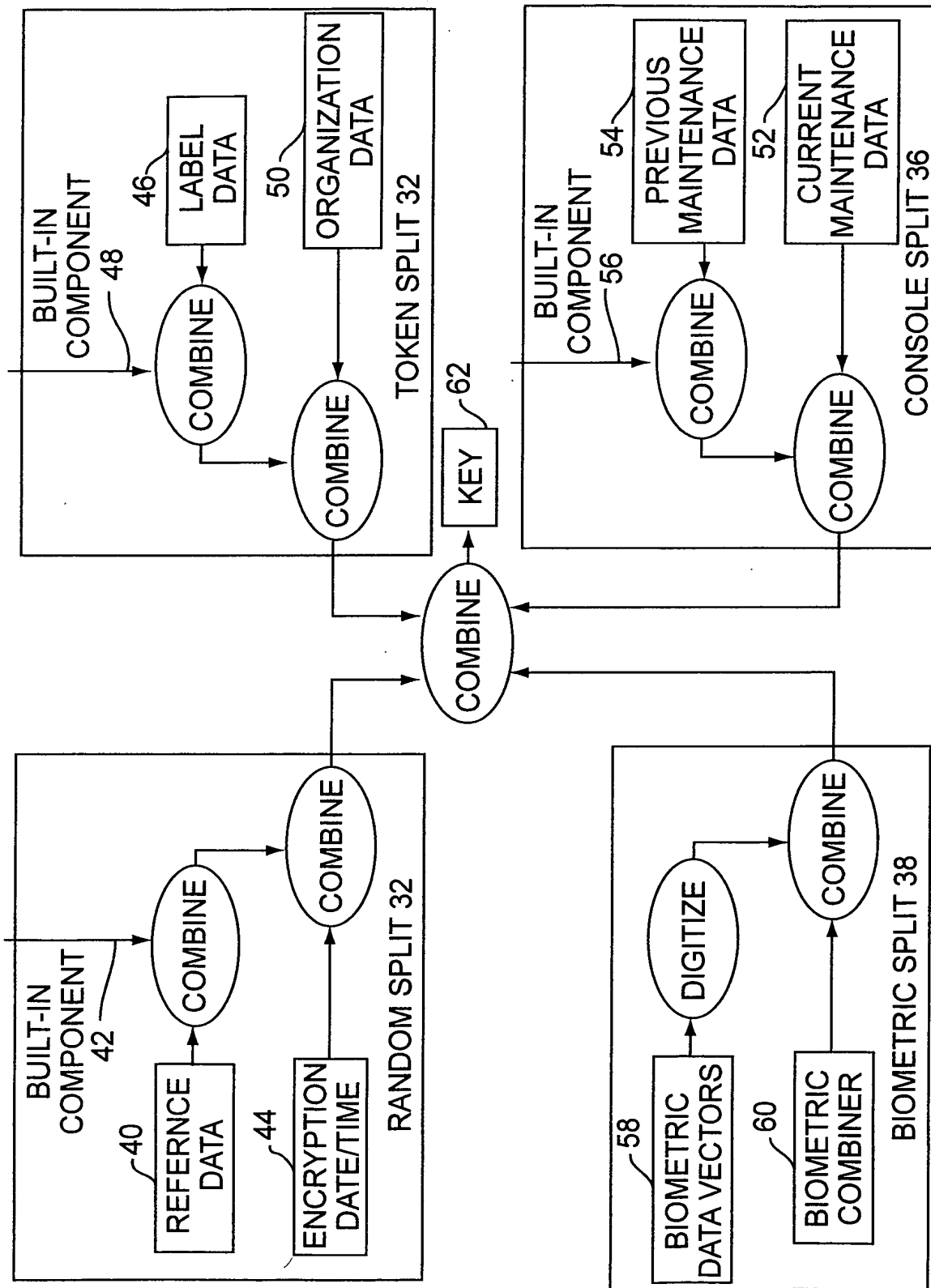


FIG. 6

7/22

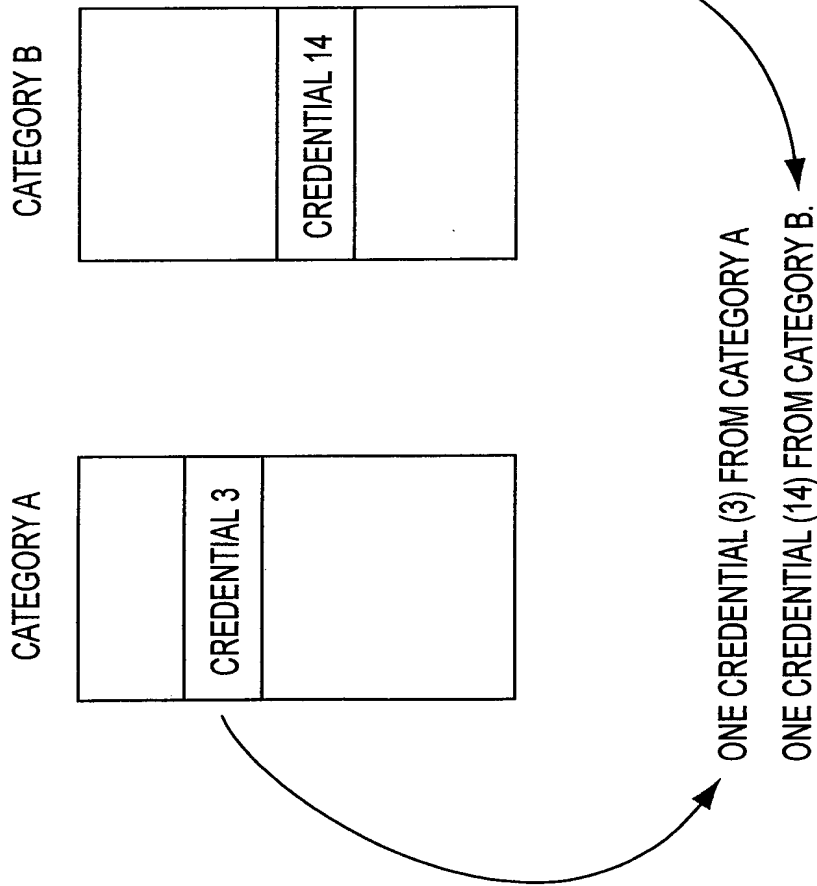
NUMBER	DECRYPT	ENCRYPT	NUMBER	DECRYPT	ENCRYPT	NUMBER	DECRYPT	ENCRYPT
1	-	-	4	↑	-	7	↓	-
2	-	↑	5	↑	↑	8	↓	↑
3	-	↓	6	↑	↓	9	↓	↓

FIG. 7

8/22

ACCESS RESTRICTED CREDENTIALS

1. DURING OBJECT ENCRYPTION, MEMBER CHOOSES WHICH CREDENTIALS TO APPLY, NO MORE THAN ONE CREDENTIAL PER CATEGORY.
2. ACCESS IS GRANTED TO DECRYPT ONLY IF READ PERMISSION (KNOWLEDGE OF PRIVATE KEY) IS AVAILABLE FOR ALL CREDENTIALS THAT WERE USED TO DECRYPT.



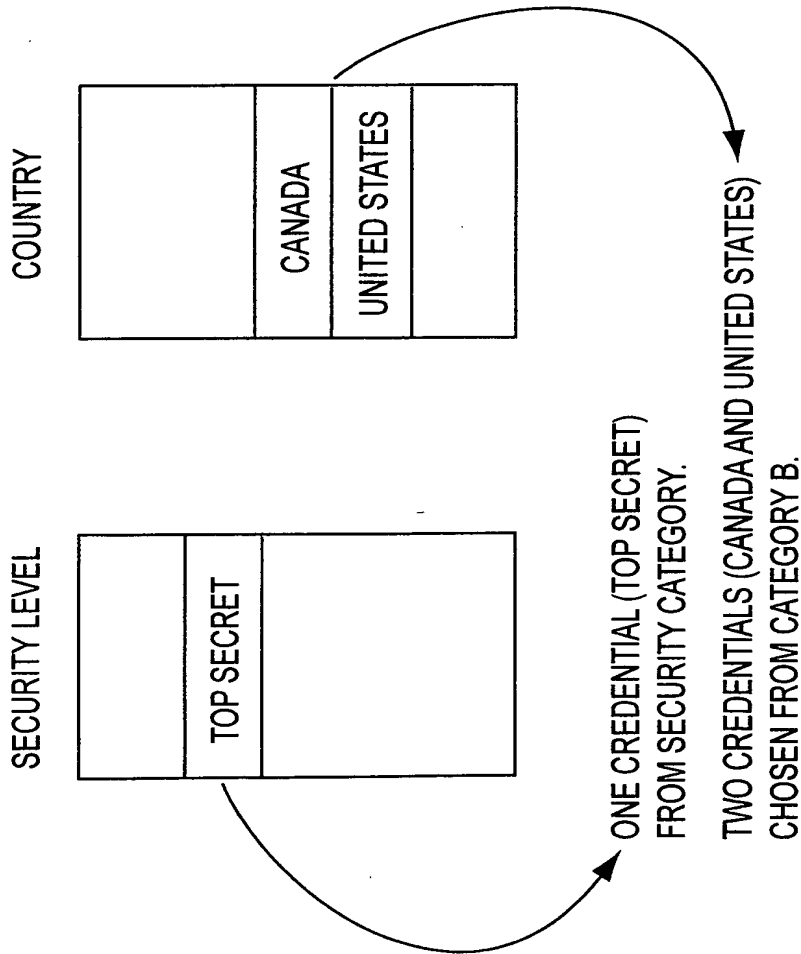
READ PERMISSION FOR BOTH CREDENTIALS
(3 AND 14) ARE NEEDED TO BE ABLE TO DECRYPT.

FIG. 8

9/22

ACCESS BROADENING CREDENTIALS

1. DURING OBJECT ENCRYPTION, MEMBER CHOOSES WHICH CREDENTIALS TO APPLY. MORE THAN ONE CREDENTIAL CAN BE SELECTED WITHIN A CATEGORY IF THAT CATEGORY IS A MULTIPLE CREDENTIAL SELECTION CATEGORY.
2. ACCESS IS GRANTED TO DECRYPT IF READ PERMISSION (KNOWLEDGE OF PRIVATE KEY) IS AVAILABLE FOR ANY ONE CREDENTIAL THAT WAS USED TO ENCRYPT IN A MULTIPLE CREDENTIAL SELECTION CATEGORY.



.....

READ PERMISSION FOR TOP SECRET AND EITHER CANADA OR US ARE NEEDED TO BE ABLE TO DECRYPT.

FIG. 9

11/22

ACCESS TYPE	SET OF AVAILABLE CREDENTIALS
1	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
2	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
3	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$
4	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
5	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
6	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$
7	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
8	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
9	$\{(\forall c \in P \exists. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \exists. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$

FIG. 11

12/22

ACCESS TYPE	xek_c	yek_c	INDEPENDENT READ VALUE	INDEPENDENT WRITE VALUE
1	$xek_c = \kappa_\lambda$	$yek_c = \kappa_\lambda$	N/A	N/A
2	$xek_c = \kappa_\lambda$	$yek_c = (H^{(0,c-1)}(yek_1)) / 2^{(h-k)}$	N/A	yek_1
3	$xek_c = \kappa_\lambda$	$yek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	N/A	yek_s
4	$xek_c = (H^{(0,c-1)}(xek_1)) / 2^{(h-k)}$	$yek_c = \kappa_\lambda$	xek_1	N/A
5	$xek_c = (H^{(0,c-1)}(xek_1)) / 2^{(h-k)}$	$yek_c = (H^{(0,c-1)}(yek_1)) / 2^{(h-k)}$	xek_1	yek_1
6	$xek_c = (H^{(0,c-1)}(xek_1)) / 2^{(h-k)}$	$yek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	xek_1	yek_s
7	$xek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	$yek_c = \kappa_\lambda$	xek_s	N/A
8	$xek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	$yek_c = (H^{(0,c-1)}(yek_1)) / 2^{(h-k)}$	xek_s	yek_1
9	$xek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	$yek_c = (H^{(s-\lambda,c)}(xek_s)) / 2^{(h-k)}$	xek_s	yek_s

FIG. 12

13/22

PROFILE ENCRYPTION

<p>ENCRYPTED PROFILE ENCRYPTION KEYS</p> $\begin{aligned} ePEK_1 &= e(PEK_1, \kappa_1) \\ ePEK_2 &= e(PEK_2, \kappa_2) \\ &\cdot \\ &\cdot \\ &\cdot \\ ePEK_{j_{max}} &= e(PEK_{j_{max}}, \kappa_{j_{max}}) \end{aligned}$	<p>ENCRYPTED CREDENTIAL PRIVATE AND PUBLIC KEY ENCRYPTION KEYS</p> $\begin{aligned} exek_1 &= e(xek_1, \kappa_1) \quad eyek_1 = e(yek_1, \kappa_1) \\ exek_2 &= e(xek_2, \kappa_2) \quad eyek_2 = e(yek_2, \kappa_2) \\ &\cdot \\ &\cdot \\ &\cdot \\ exek_{j_{max}} &= e(xek_{j_{max}}, \kappa_{j_{max}}) \quad eyek_{j_{max}} = e(yek_{j_{max}}, \kappa_{j_{max}}) \end{aligned}$
<p>ENCRYPTED PROFILE</p> $eProfile = e(Profile, PEK)$	<p>ENCRYPTED CREDENTIAL PRIVATE AND PUBLIC KEYS</p> $\begin{aligned} ex_1 &= e(x_1, xek_{x_1}) \quad ey_1 = e(y_1, yek_{y_1}) \\ ex_2 &= e(x_2, xek_{x_2}) \quad ey_2 = e(y_2, yek_{y_2}) \\ &\cdot \\ &\cdot \\ &\cdot \\ ex_n &= e(x_n, xek_{x_n}) \quad ey_n = e(y_n, yek_{y_n}) \end{aligned}$

FIG. 13

14/22

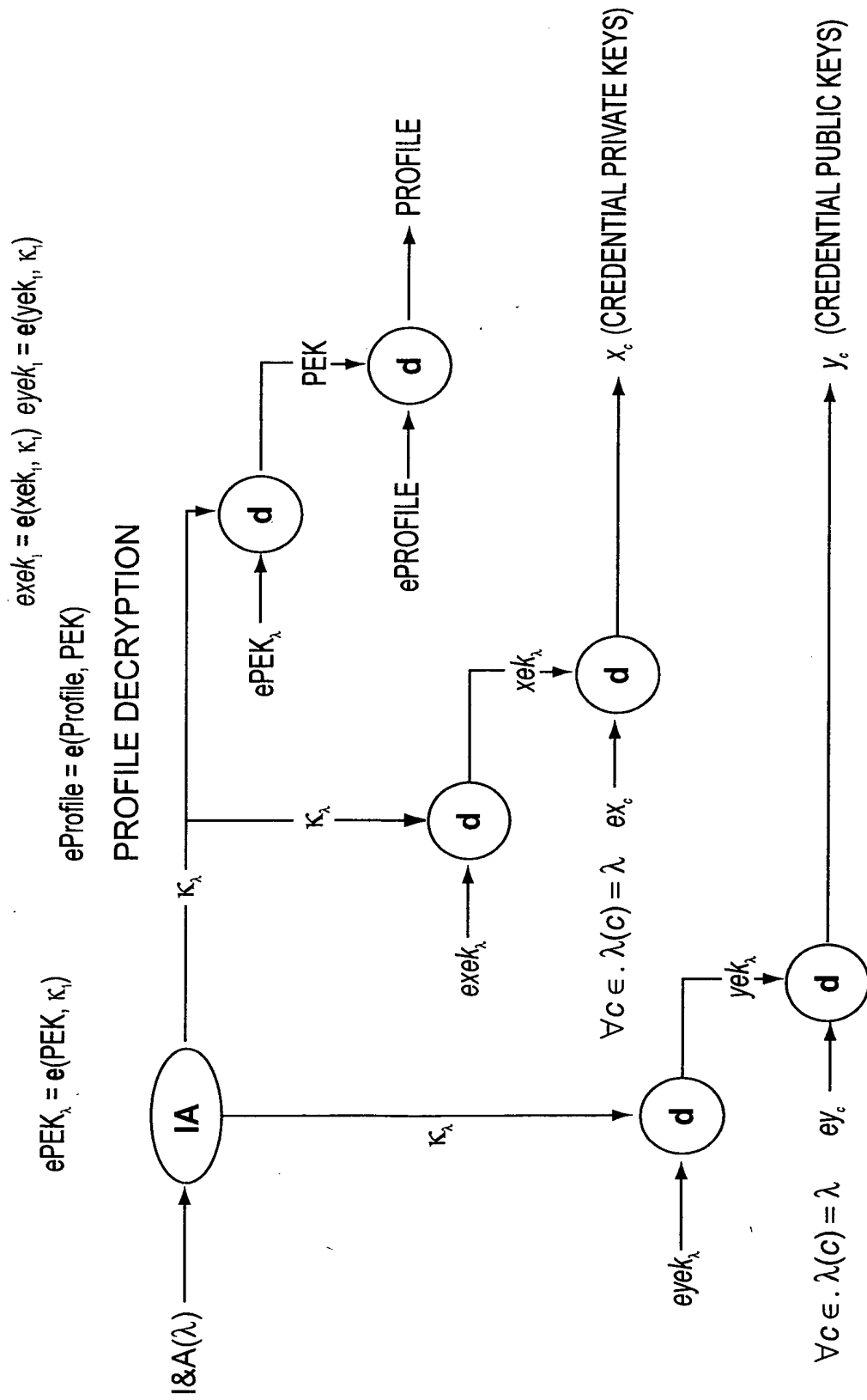


FIG. 14

15/22

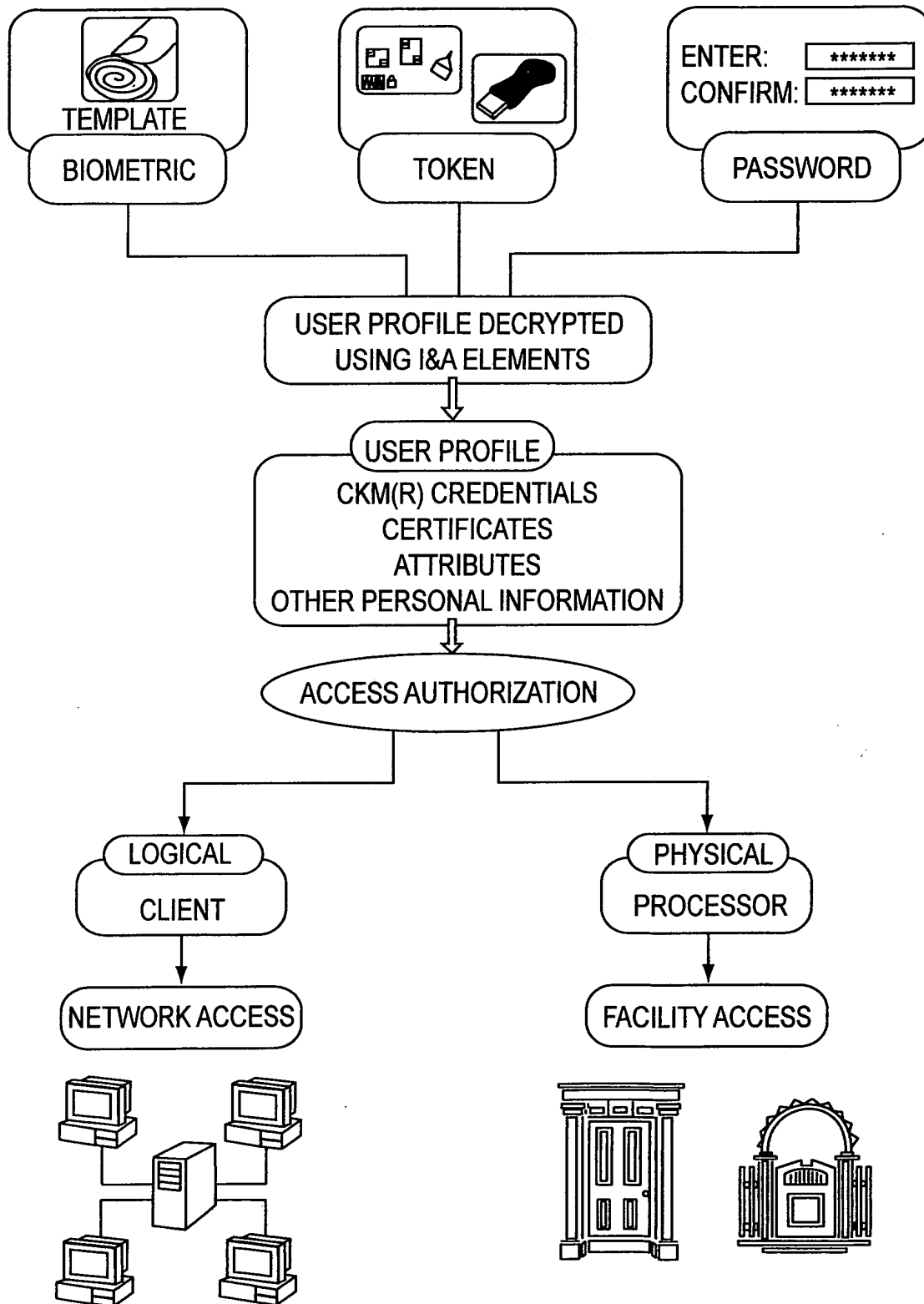


FIG. 15

16/22

PASSWORD AUTHENTICATION TO A HARDWARE TOKEN

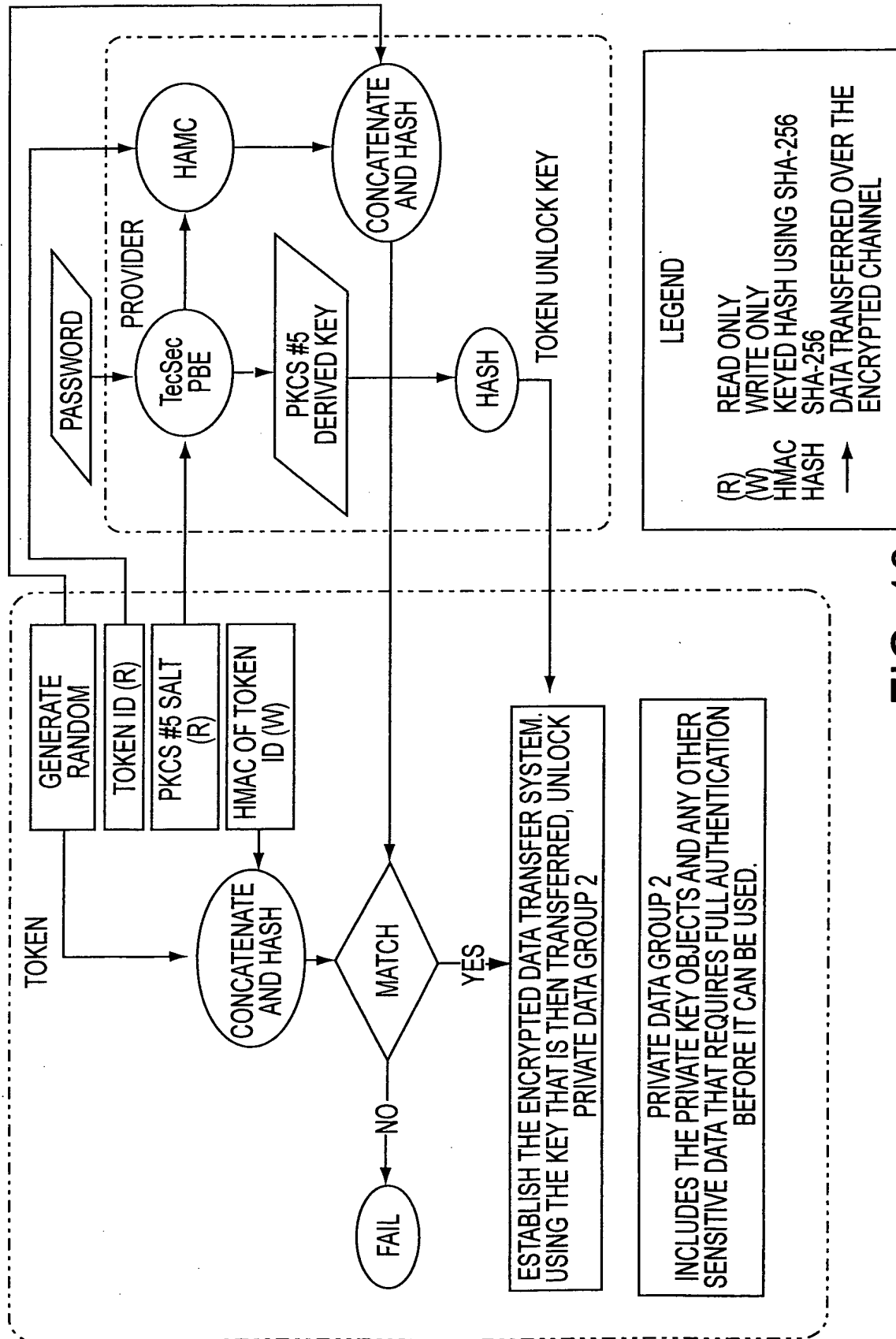
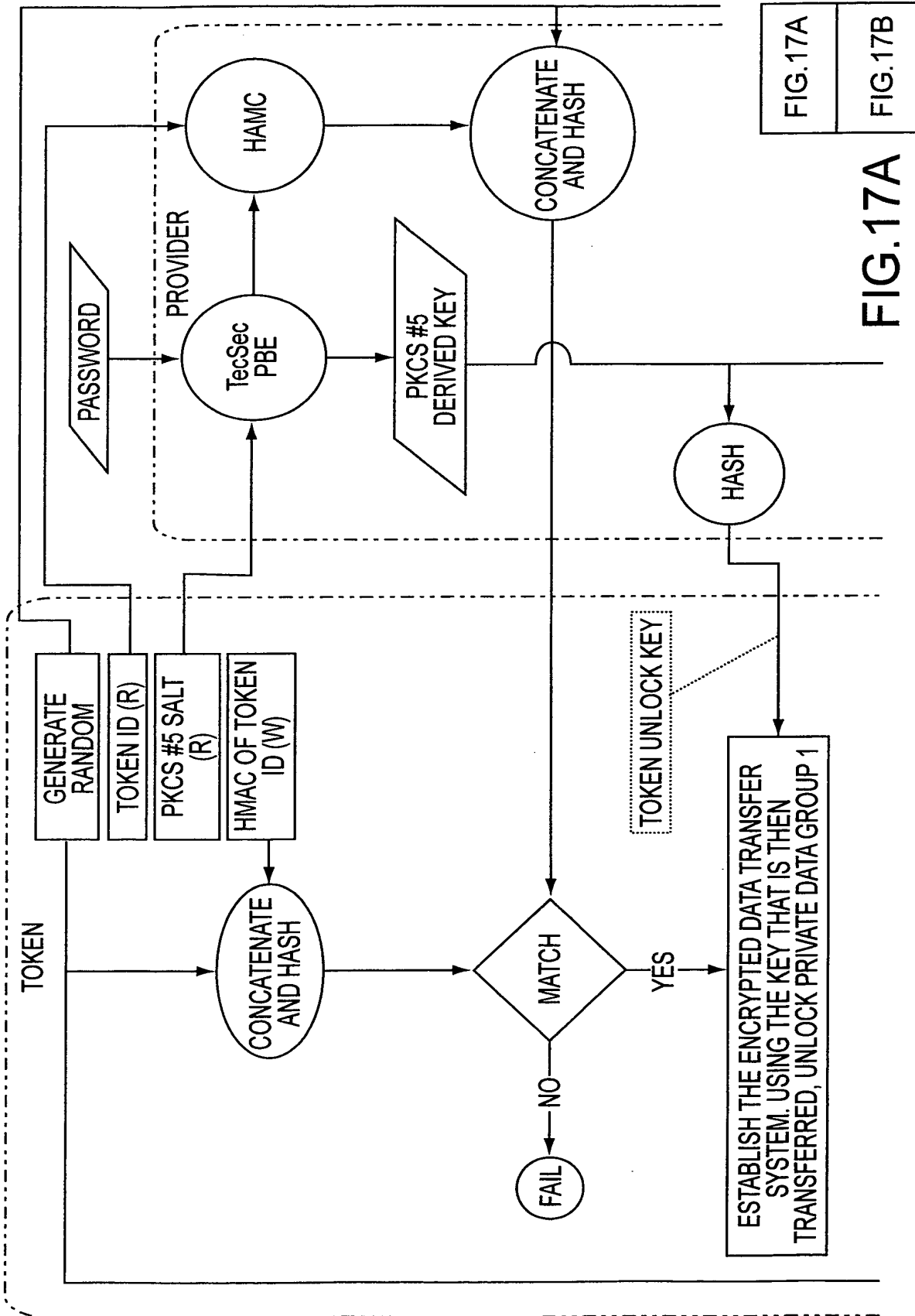


FIG. 16

17A/22

PASSWORD AND BIOMETRIC AUTHENTICATION TO A HARDWARE TOKEN



17B/22

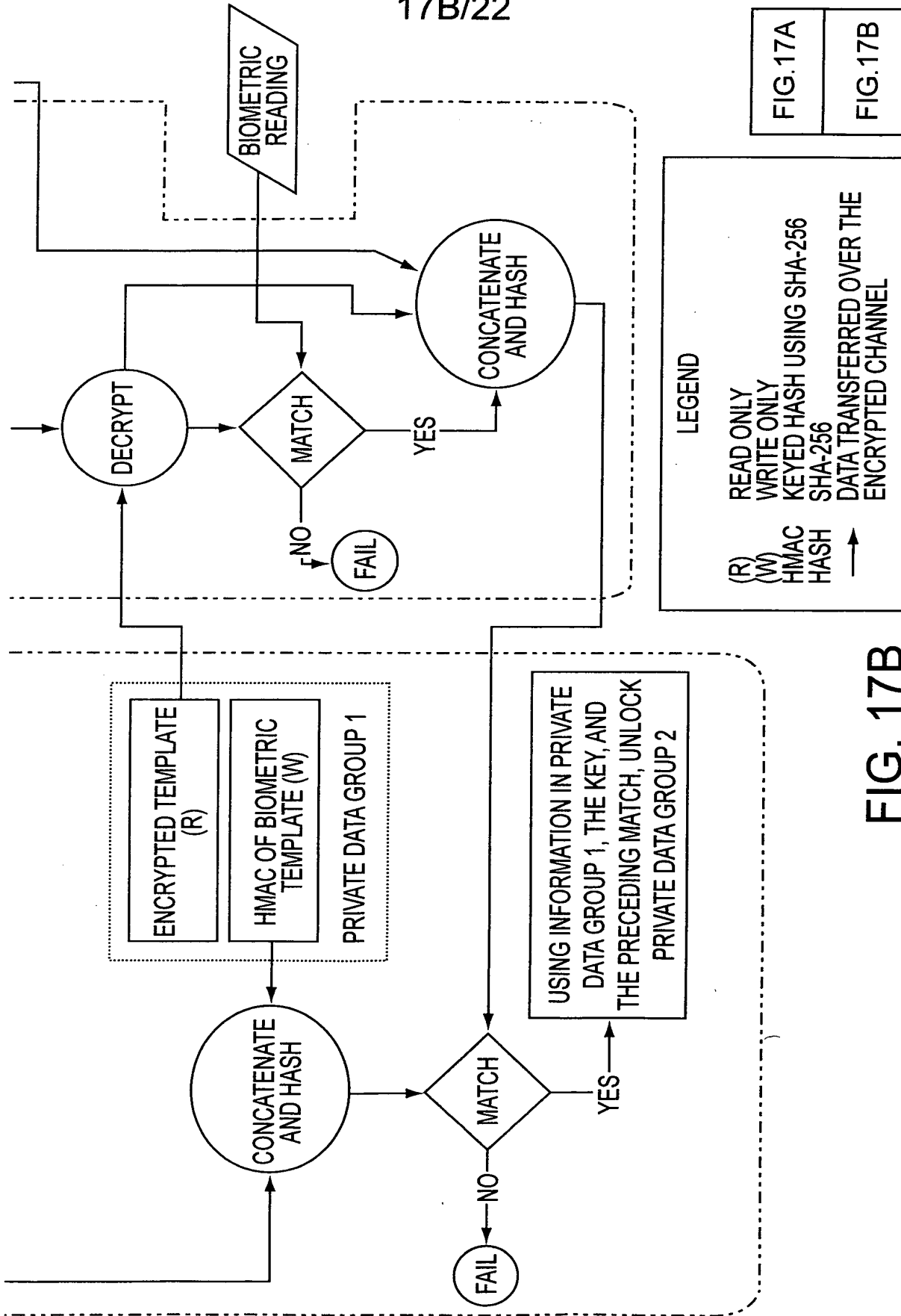
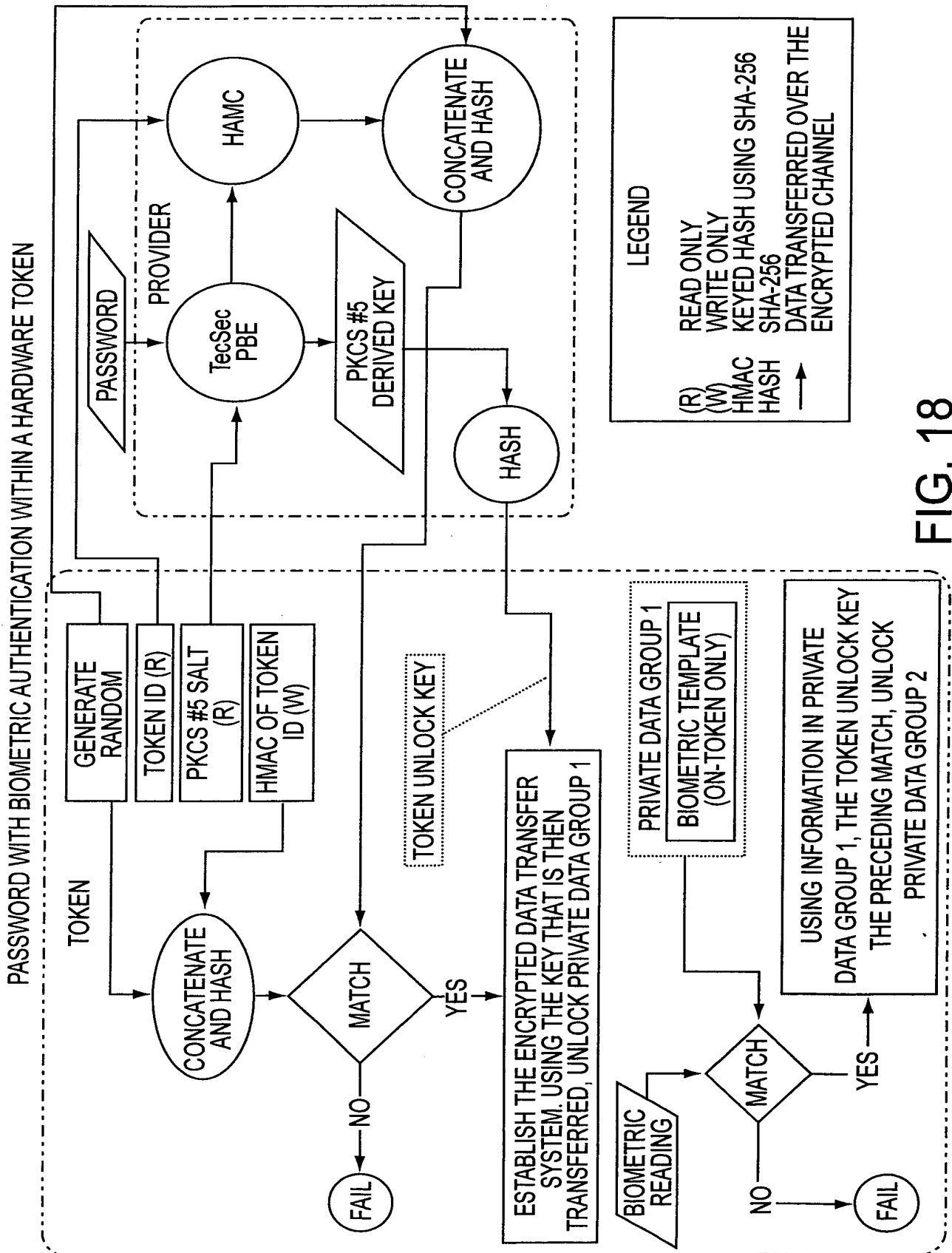


FIG. 17B

18/22



19/22

MESSAGE TRANSMISSION FROM CLIENT TO TOKEN WITH MESSAGE NUMBERING

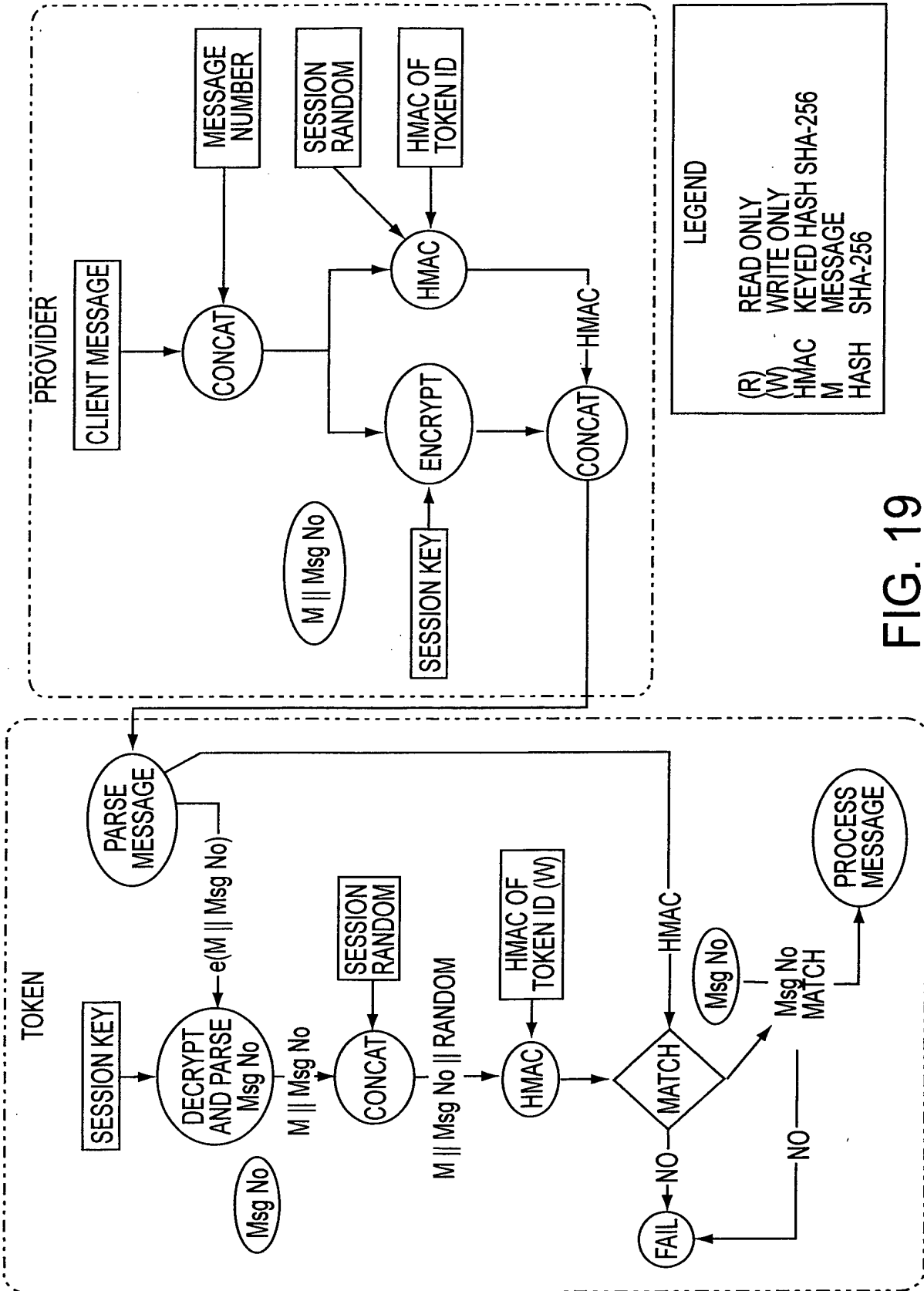


FIG. 19

20/22

MESSAGE TRANSMISSION FROM CLIENT TO TOKEN WITH NO MESSAGE NUMBER

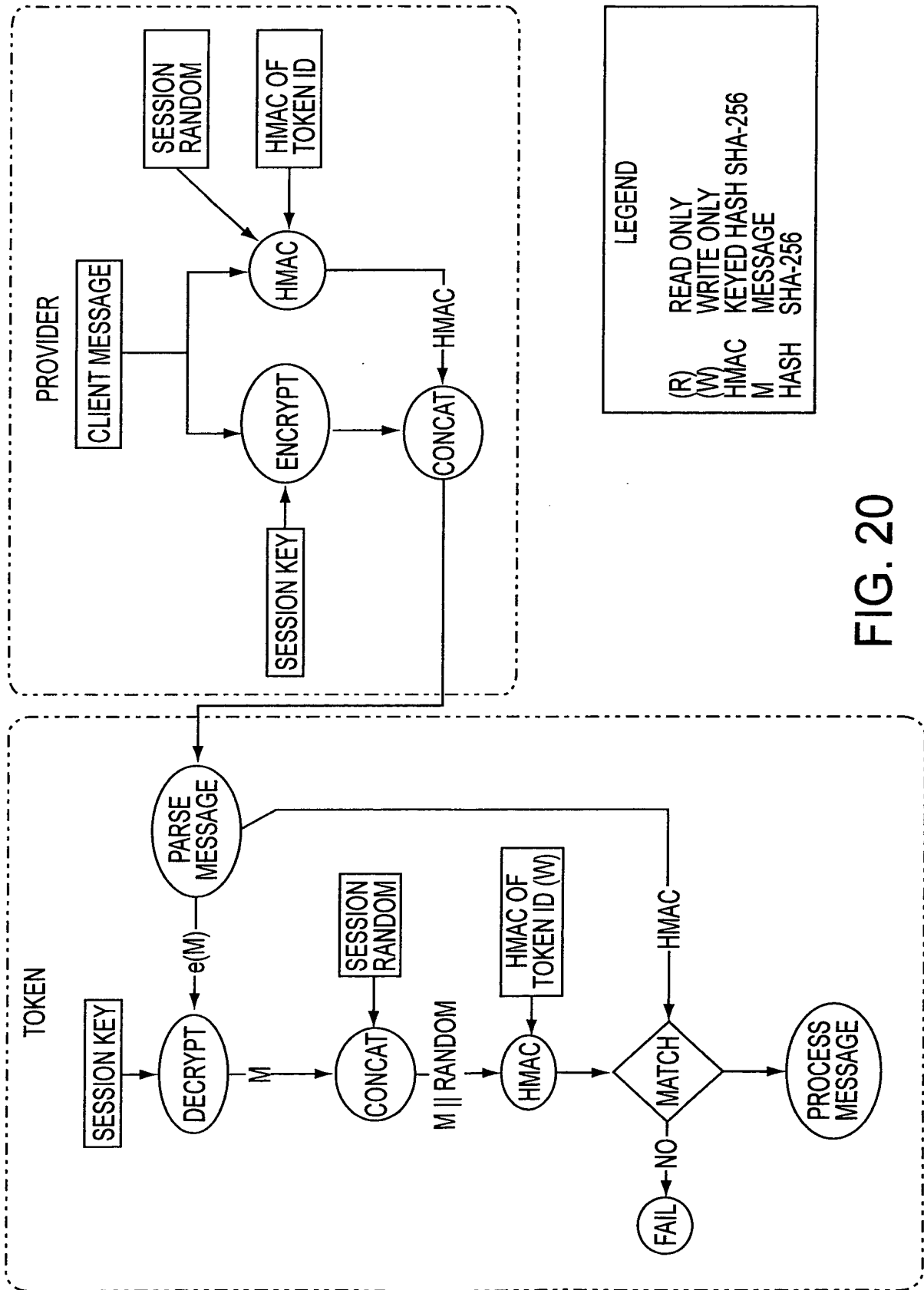


FIG. 20

21/22

KEY DERIVATION FUNCTION

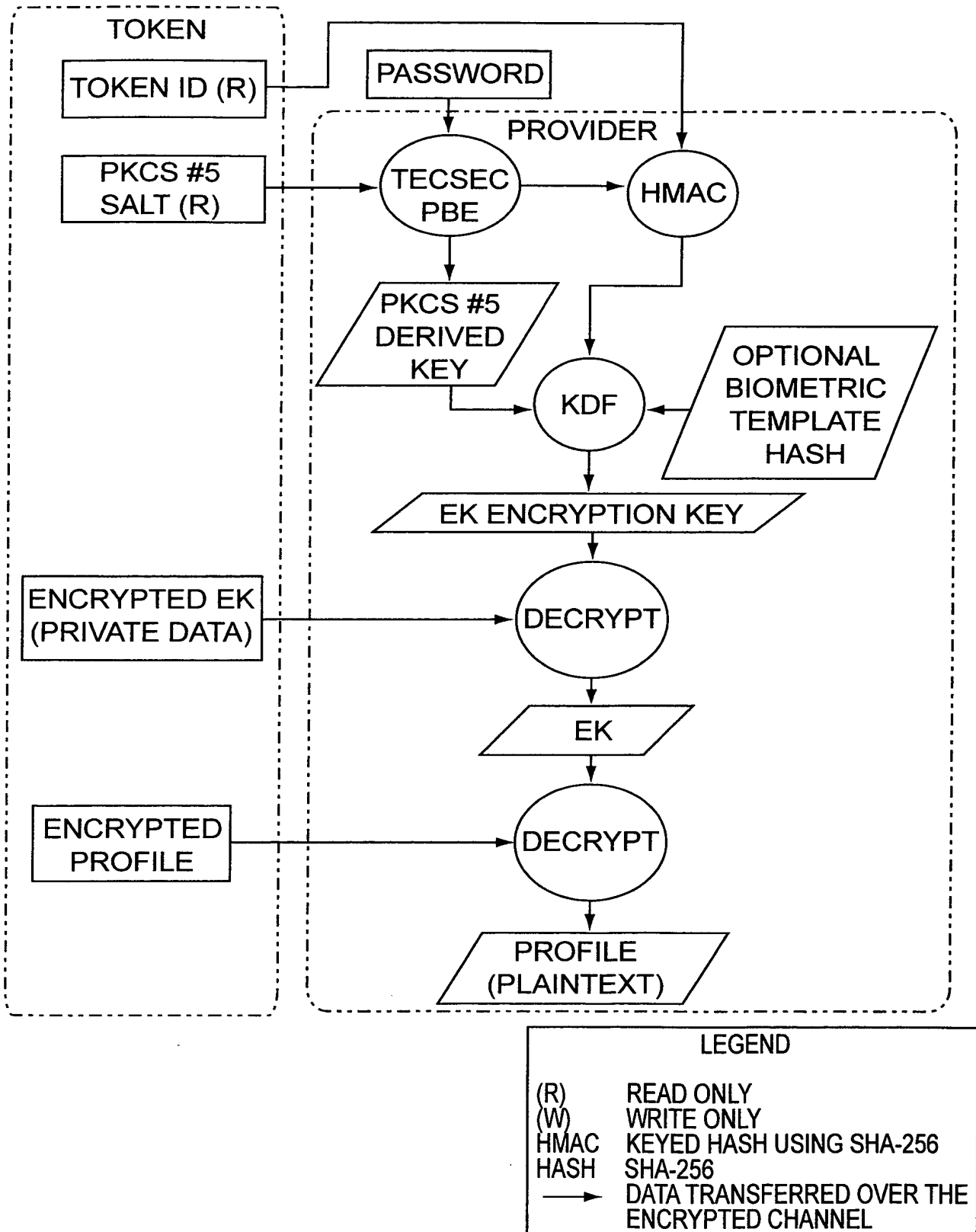


FIG. 21

22/22

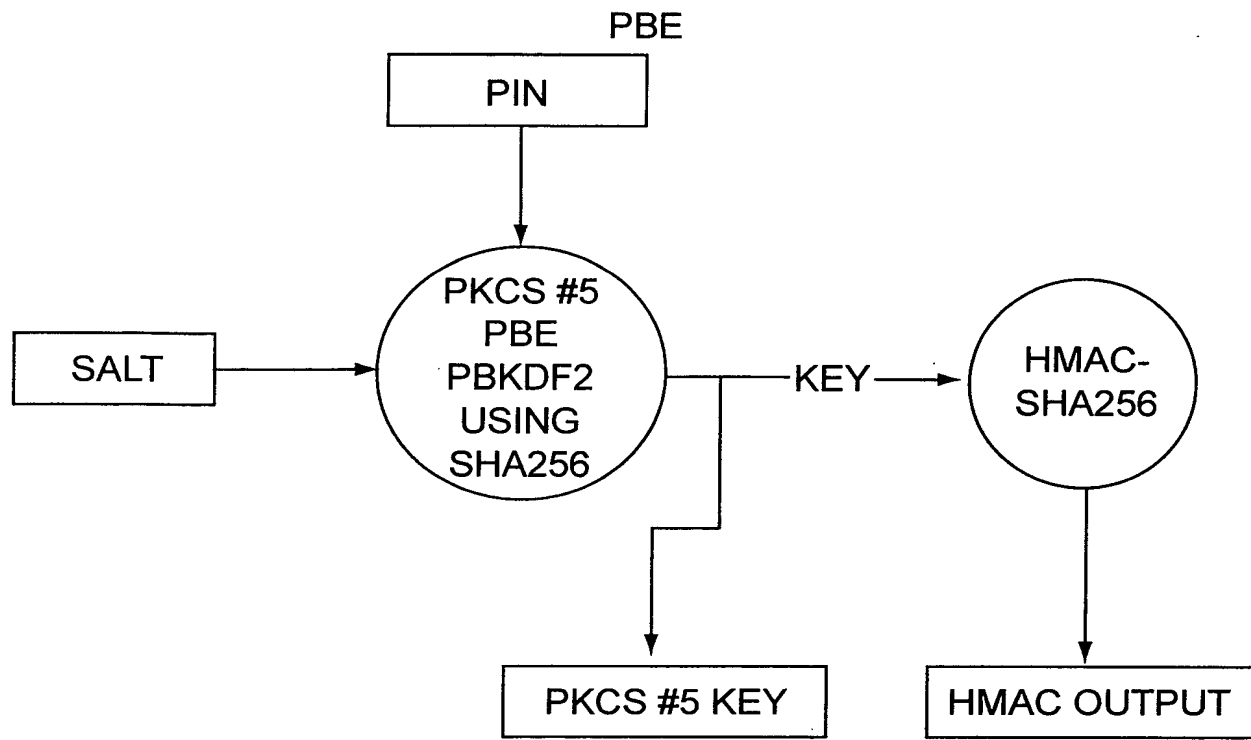


FIG. 22